REMARKS

Claims 1-36 are pending in this application. The Office Action rejects claims 1, 2, 6-8, 10-12, and 15 under 35 U.S.C. § 102(e) over U.S. Patent No. 5,987,011 to Toh; claim 16 under 35 U.S.C. § 102(e) over U.S. Patent No. 6,304,556 B1 to Haas; claims 25 and 26 under 35 U.S.C. § 102(b) over U.S. Patent No. 5,473,599 to Li; and claims 27-35 under 35 U.S.C. § 102(e) over U.S. Patent No. 6,618,377 B1 to Miriyala. In addition, on the basis of under 35 U.S. C. § 103, the Office Action also rejects claims 3, 4, 9 and 13 over Toh in view of U.S. Patent No. 6,529,515 B1 to Raz; claims 5 and 14 over Toh in view of the Applied Cryptography text by Schneier; claims 17-23 as over Li in view of U.S. Patent No. 4,947,430 to Chaum; and claim 36 over Miriyala in view of U.S. Patent No. 5,968,176 to Nessett.

Applicant traverses the rejections, amends the claims, and submits the enclosed Request for Continued Examination. Applicant amends claims 1, 3, 6-7, 12, 16-17, 22, and 24-36 to improve form and to more clearly set forth the claimed subject matter, i.e., methods, routers, software, and networks that react to a determination that an untrusted party has gained control of a router in a network.

In general the application relates to routers, methods, and software for use in ad hoc networks that help prevent potential damage arising from an untrusted party gaining control of a router. In general, router controlling parties can be divided into two sets of parties, trusted and untrusted. For example, in a military setting, trusted parties may include friendly forces and untrusted parties may include enemy forces. In a civilian scenario, untrusted parties may include, e.g., thieves and hackers. If an untrusted party gains control of a router, the router is "compromised." An untrusted party can use a compromised router for initiating denial of service

attacks and other forms of malicious activity. To prevent such activity, once informed of the change of control of a compromised router, the remaining routers in the network excise or cut-off the compromised router from the network. Thereafter, the remaining routers cease sending data packets to the compromised router and ignore data packets received from the compromised router.

None of the references cited in the Office Action relate to reactions to the determination that an untrusted party has gained control of a router in the network, a limitation included in all independent claims. In fact, the references are entirely silent with respect to reacting to changes in party router control. Instead, the primary references relate to reacting to router failure or routing environment changes, e.g., a target router moving out of range. Reacting to a change in control is a patentably distinct activity. Therefore, no reference or combination of references teaches or suggests the subject matter of the pending claims.

Applicant respectfully submits that all pending claims are patentable over the references, either alone, or in combination. Applicant requests reconsideration and withdrawal of the §102 and §103 rejections.

CONCLUSION

In view of the foregoing amendments and remarks, Applicant respectfully requests favorable reconsideration and passage to issue of the present application.

If there are any fees due in connection with the filing of this response, please charge the fees to our Deposit Account No. 18-1945 under Order No. BBNT-P01-007. If an extension of time under 37 C.F.R. § 1.136 not accounted for above is required, such an extension is requested and the fee should also be charged to our Deposit Account.

Dated: November 9, 2004

Respectfully submitted,

By _____

Edward A. Gordon
Registration No.: 54,130
ROPES & GRAY LLP
One International Place
Boston, Massachusetts 02110-2624
(617) 951-7000
(617) 951-7050 (Fax)
Attorneys/Agents For Applicant